The US-CERT Cyber Security Bulletin provides a summary of new and updated vulnerabilities, exploits, trends, and malicious code that have recently been openly reported. Information in the Cyber Security Bulletin is a compilation of open source and US-CERT vulnerability information. As such, the Cyber Security Bulletin includes information published by sources outside of US-CERT and *should* ***not*** *be considered the result of US-CERT analysis or as an official report of US-CERT*. Although this information does reflect open source reports, it is not an official description and should be used for informational purposes only. The intention of the Cyber Security Bulletin is to serve as a comprehensive directory of pertinent vulnerability reports, providing brief summaries and additional sources for further investigation.

Vulnerabilities

The tables below summarize vulnerabilities that have been reported by various open source organizations or presented in newsgroups and on web sites. **Items in bold designate updates that have been made to past entries.** Entries are grouped by the operating system on which the reported software operates, and vulnerabilities which affect both Windows and Unix/ Linux Operating Systems are included in the Multiple Operating Systems table. *Note*, entries in each table are not necessarily vulnerabilities *in* that operating system, but vulnerabilities in software which operate on some version of that operating system.

Entries may contain additional US-CERT sponsored information, including Common Vulnerabilities and Exposures (CVE) numbers, National Vulnerability Database (NVD) links, Common Vulnerability Scoring System (CVSS) values, Open Vulnerability and Assessment Language (OVAL) definitions, or links to US-CERT Vulnerability Notes. Metrics, values, and information included in the Cyber Security Bulletin which has been provided by other US-CERT sponsored programs, is prepared, managed, and contributed by those respective programs. CVSS values are managed and provided by the US-CERT/ NIST National Vulnerability Database. Links are also provided to patches and workarounds that have been provided by the product’s vendor.

The Risk levels are defined below:

High - Vulnerabilities will be labeled “High” severity if they have a CVSS base score of 7.0-10.0.

Medium - Vulnerabilities will be labeled “Medium” severity if they have a base CVSS score of 4.0-6.9.

Low - Vulnerabilities will be labeled “Low” severity if they have a CVSS base score of 0.0-3.9.

Note that scores provided prior to 11/9/2005 are approximated from only partially available CVSS metric data. Such scores are marked as "Approximated" within NVD. In particular, the following CVSS metrics are only partially available for these vulnerabilities and NVD assumes certain values based on an approximation algorithm: AccessComplexity, Authentication, ConfImpact of 'partial', IntegImpact of 'partial', AvailImpact of 'partial', and the impact biases.

Windows Operating Systems Only

Vendor & Software Name	Description	Common Name	CVSS	Resources

Adobe Graphics Server 2.1, Document Server 6.0	A vulnerability has been reported in Graphics Server and Document Server that could let remote malicious users execute arbitrary code. Adobe Currently we are not aware of any exploits for these vulnerabilities.	Adobe Graphics Server and Document Server Arbitrary Code Execution CVE-2006-1182	Not Available	Adobe, Security Advisory 332989, March 14, 2006
Apache Software Foundation Log4net 1.2.9	A vulnerability has been reported in Log4net that could let remote malicious users cause a Denial of Service vulnerability. Apache Software Foundation Currently we are not aware of any exploits for these vulnerabilities.	Apache Log4net Denial of Service Vulnerability CVE-2006-0743	2.3	Secunia, Advisory: SA19241, March 14, 2006
Apache Software Foundation mod_python 3.2.7	A directory traversal vulnerability has been reported in mod_python that could let local malicious users execute arbitrary code. Apache Software Foundation mod_python 3.2.8 There is no exploit code required.	mod_python Arbitrary Code Execution CVE-2006-1095	4.9	Security Tracker, Alert ID: 1015764, March 14, 2006
ASP Portal 3.0.0 and prior	Multiple vulnerabilities have been reported in ASP Portal that could let remote malicious perform Cross-Site Scripting or SQL injection. ASP Portal 3.1.1 There is no exploit code required.	ASP Portal Cross-Site Scripting or SQL Injection	Not Available	Secunia, Advisory: SA19247, March 15, 2006
EFS Software Easy File Sharing Web Server 3.2	An input validation vulnerability has been reported in Easy File Sharing Web Server that could let remote malicious users conduct Cross-Site Scripting or cause a Denial of Service. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Easy File Sharing Web Server Cross-Site Scripting or Denial of Service CVE-2006-1159 CVE-2006-1160	3.3 (CVE-2006-1159) 2.3 (CVE-2006-1160)	Secunia, Advisory: SA19178, March 10, 2006
Gemini Gemini 2.0	A vulnerability has been reported in Gemini that could let remote malicious users conduct Cross-Site Scripting. No workaround or patch available at time of publishing. There is no exploit code required.	Gemini Cross-Site Scripting CVE-2006-1239	Not Available	Secunia, Advisory: SA19049, March 14, 2006
Hosting Controller Hosting Controller 6.1 HotFix 2.9	A vulnerability has been reported in Hosting Controller that could let remote malicious users perform SQL injection. No workaround or patch available at time of publishing. There is no exploit code required.	Hosting Controller SQL Injection CVE-2006-1229	2.3	Secunia, Advisory: SA19191, March 10, 2006
Ipswitch IMail Server 2006, Secure Server 2006 Collaboration Suite Standard 2006, Premium 2006	A buffer overflow vulnerability has been reported in IMail Secure Server and Collaboration Suite, IMAP fetch command, that could let remote malicious users cause a Denial of Service or execute arbitrary code. Ipswitch Server 2006.03 Ipswitch Secure Server 2006.03 Ipswitch Collaboration Suite Standard 2006.03 Ipswitch Collaboration Suite Premium 2006 .03	Ipswitch IMail Server and Collaboration Suite Denial of Service or Arbitrary Code Execution CVE-2005-3526	4.2	Secunia Advisory: SA19168, March 10, 2006

	Currently we are not aware of any exploits for these vulnerabilities.			
JiRos JiRos Banner Experience & Professional 1.0 & prior	A vulnerability has been reported in Banner Experience Pro, 'addadmin.asp,' that could let remote malicious users bypass security restrictions. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for these vulnerabilities.	Jiros Banner Experience Pro Security Restriction Bypassing CVE-2006-1213	7	Security Focus, ID: 17060, March 9, 2006
Kerio MailServer prior to 6.1.3 P1	A vulnerability has been reported in Kerio Mailserver that could let remote malicious users cause a Denial of Service. Kerio Mailserver 6.1.3 P1 Currently we are not aware of any exploits for this vulnerability.	Kerio MailServer Denial of Service CVE-2006-1158	3.3	Security Tracker, Alert ID: 1015748, March 10, 2006
Macrovision SafeDisc	A vulnerability has been reported in SafeDisc that could let local malicious users obtain elevated privileges. No workaround or patch available at time of publishing. There is no exploit code required.	SafeDisc Privilege Elevation CVE-2006-1197	7	Security Focus, ID: 17070, March 11, 2006
Microsoft Microsoft Office 2000, 2003 Professional, 2003 Small Business, 2003 Standard, 2003 Student, 2003 Student and Teacher, 2004 for Mac, X for Mac, XP Microsoft Works Suite 2001 to 2006 Microsoft Excel, Excel Viewer, Outlook, PowerPoint and Word various versions	Multiple vulnerabilities have been reported in Microsoft Office that could let remote malicious users execute arbitrary code. Microsoft Avaya Currently we are not aware of any exploits for these vulnerabilities.	Microsoft Office Multiple Arbitrary Code Execution CVE-2005-4131 CVE-2006-0009 CVE-2006-0028 CVE-2006-0029 CVE-2006-0030 CVE-2006-0031	2.8 (CVE-2005-4131) 5.6 (CVE-2006-0009) 5.6 (CVE-2006-0028) 5.6 (CVE-2006-0029) 5.6 (CVE-2006-0030) 5.6 (CVE-2006-0031)	Microsoft, Security Bulletin MS06-012, March 14, 2006 Cyber Security Alert SA06-073A Technical Cyber Security Alert TA06-073A US-CERT VU#339878, VU#235774, VU#123222, VU#642428, VU#104302, VU#682820
Microsoft Windows XP SP1, Server 2003, and Server 2003 for Itanium Systems	A vulnerability has been reported in Windows, default ACL settings, that could let remote malicious users obtain elevated privileges. Microsoft Avaya There is no exploit code required.	Microsoft Windows Privilege Elevation CVE-2006-0023	2.9	Microsoft, Security Bulletin MS06-011, March 14, 2006
Zone Labs ZoneAlarm 6.1.744.000	A vulnerability has been reported in ZoneAlarm that could let local malicious users execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required.	ZoneAlarm Arbitrary Code Execution CVE-2006-1221	5.6	Security Tracker, Alert ID: 1015743, March 9, 2006

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Description	Common Name	CVSS	Resources

Apple Mac OS X Server 10.4-10.4.5, 10.3-10.3.9, 10.2-10.2.8, 10.1-10.1.5, 10.0-10.0.4, Mac OS 0.4-10.4.5, 10.3-10.3.9, 10.2-10.2.8, 10.1-10.1.5, 10.0-10.0.4	A heap overflow vulnerability has been reported in the 'mach_msg_send()' function of the kernel, which could let a malicious user cause a Denial of Service and possibly compromise a system. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Apple Mac OS X Kernel MACH_MSG _SEND Heap Overflow CVE-2006-1220	4.9	Security Focus, Bugtraq ID: 17056, March 9, 2006
Apple Mac OS X Server 10.4-10.4.5, Mac OS X 10.4-10.4.5	Multiple vulnerabilities have been reported: a vulnerability was reported in JavaScript because in certain circumstances because it is possible to bypass the same-origin policy; a buffer overflow vulnerability was reported in Mail due to a boundary error, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported in Safari/LaunchServices due to an error which could lead to the execution of a malicious file. Updates available Currently we are not aware of any exploits for these vulnerabilities.	Mac OS X Security Update CVE-2006-0396 CVE-2006-0397 CVE-2006-0398 CVE-2006-0399 CVE-2006-0400	7 (CVE-2006-0396) 5.6 (CVE-2006-0397) 5.6 (CVE-2006-0398) 5.6 (CVE-2006-0399) 7 (CVE-2006-0400)	Apple Security Update, APPLE-SA-2006-03-13, March 13, 2006
BlueZ Project hcidump 1.29	A remote Denial of Service vulnerability has been reported in '12cap.c' due to an error when handling L2CAP (Logical Link Control and Adaptation Layer Protocol) layer. Ubuntu **Debian** A Proof of Concept exploit script, hcidump-crash.c, has been published.	hcidump Bluetooth L2CAP Remote Denial of Service CVE-2006-0670	**2.3**	Secunia Advisory: SA18741, February 8, 2006 Ubuntu Security Notice, USN-256-1, February 21, 2006 **Debian Security Advisory, DSA 990-1, March 10, 2006**
bzip2 bzip2 1.0.2	A remote Denial of Service vulnerability has been reported when processing malformed archives. Ubuntu Mandriva TurboLinux SUSE OpenPKG RedHat FreeBSD Conectiva Debian SGI IPCop FedoraLegacy **SGI** Currently we are not aware of any exploits for this vulnerability.	bzip2 Remote Denial of Service CVE-2005-1260	3.3	Ubuntu Security Notice, USN-127-1, May 17, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005: 091, May 19, 2005 Turbolinux Security Advisory, TLSA-2005-60, June 1, 2005 SUSE Security Summary Report, SUSE-SR:2005:015, June 7, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.008, June 10, 2005 RedHat Security Advisory, RHSA-2005: 474-15, June 16, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:14, June 29, 2005 Conectiva Linux Announce -ment, CLSA-2005:972, July 6, 2005 Debian Security Advisory,

				DSA 741-1, July 7, 2005 SGI Security Advisory, 20050605 -01-U, July 12, 2005 Security Focus, Bugtraq ID: 13657, August 26, 2005 Fedora Legacy Update Advisory, FLSA:158801, November 14, 2005 **SGI Security Advisory, 20060301-01-U, March 8, 2006**
bzip2 bzip2 1.0.2 & prior	A vulnerability has been reported when an archive is extracted into a world or group writeable directory, which could let a malicious user modify file permissions of target files. Ubuntu Mandriva Debian TurboLinux OpenPKG RedHat FreeBSD Conectiva SGI FedoraLegacy Mandriva **SGI** There is no exploit code required.	BZip2 File Permission Modification CVE-2005-0953	4.9	Security Focus, 12954, March 31, 2005 Ubuntu Security Notice, USN-127-1, May 17, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005: 091, May 19, 2005 Debian Security Advisory, DSA 730-1, May 27, 2005 Turbolinux Security Advisory, TLSA-2005-60, June 1, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.008, June 10, 2005 RedHat Security Advisory, RHSA-2005 :474-15, June 16, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:14, June 29, 2005 Conectiva Linux Announcement, CLSA-2005:972, July 6, 2005 SGI Security Advisory, 20050605- 01-U, July 12, 2005 Fedora Legacy Update Advisory, FLSA:158801, November 14, 2005 Mandriva Security Advisory, MDKSA-2006:026, January 30, 2006 **SGI Security Advisory, 20060301-01-U, March 8, 2006**
CGI::Session CGI::Session 4.03	Several vulnerabilities have been reported: a vulnerability was reported due to the insecure default read permissions on files created by 'Driver::file,' 'Driver::db_file,' and 'Driver::sqlite,' which could let a remote malicious user obtain sensitive information; and a	CGI::Session Insecure File Permissions	Not Available	Secunia Advisory: SA19211, March 13, 2006

	vulnerability was reported in the 'cgisess.db' session file that is created by the 'Driver::db_file' in the same directory as the CGI script, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through use of a web client.			
Crossfire Crossfire 1.9 , 1.8	A buffer overflow vulnerability has been reported in 'request.c' due to an error in the 'SetUp()' function when handling the 'setup' command, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit script, crossfire_bof_exp.c, has been published.	CrossFire Remote Buffer Overflow CVE-2006-1236	7	Secunia Advisory: SA19237, March 14, 2006
DokuWiki DokuWiki 2005.9.22, 2004-10-19, 2004-09-30, 2004-09-25, 2004-09-12, 2004-08-22, 2004-08-15a, 2004-08-15, 2004-08-08, 2004-07-25, 2004-07-21	A Cross-Site Scripting vulnerability has been reported in Mediamanager due to an unspecified input validation error when handling EXIF data, which could let a remote malicious user execute arbitrary HTML and script code. Updates available Vulnerability can be exploited through use of a web client.	DokuWiki Cross-Site Scripting CVE-2006-1165	2.3	Security Focus, Bugtraq ID: 17065, March 10, 2006
Firebird Firebird 1.5-1.5.2	A buffer overflow vulnerability has been reported in 'Inet_server' due to a failure due to insufficient bounds checking prior to copying to an insufficiently-sized memory buffer, which could let a malicious user execute arbitrary code. Updates available A Proof of Concept exploit has been published.	Firebird Buffer Overflow CVE-2006-1240 CVE-2006-1241	Not Available	Security Focus Bugtraq ID: 17077, March 13, 2006
Freeciv Freeciv 2.0.7	A remote Denial of Service vulnerability has been reported in 'common/packets.c' due to an error when handling the packet length. Update available Mandriva **Debian** **Gentoo** A Proof of Concept exploit script , freecivdos.zip, has been published.	Freeciv Remote Denial of Service CVE-2006-0047	3.3	Secunia Advisory: SA19120, March 6, 2006 Mandriva Linux Security Advisory MDKSA-2006:053, March 7, 2006 **Debian Security Advisory, DSA-994-1, March 13, 2006** **Gentoo Linux Security Advisory, GLSA 200603-11, March 16, 2006**

GNU Mailman 2.1-2.1.5, 2.0-2.0.14	A remote Denial of Service vulnerability has been reported in 'Scrubber.py' due to a failure to handle exception conditions when Python fails to process an email file attachment that contains utf8 characters in its filename. Mandriva SuSE Ubuntu Debian RedHat **Trustix** There is no exploit code required.	GNU Mailman Attachment Scrubber UTF8 Filename Remote Denial of Service CVE-2005-3573	2.3	Secunia Advisory: SA17511, November 14, 2005 Mandriva Linux Security Advisory, MDKSA-2005:222, December 2, 2005 SUSE Security Summary Report, SUSE-SR:2006:001, January 13, 2006 Ubuntu Security Notice, USN-242-1 January 16, 2006 Debian Security Advisory, DSA-955-1, January 25, 2006 RedHat Security Advisory, RHSA-2006:0204-10, March 7, 2006 **Trustix Secure Linux Security Advisory #2006-0012, March 10, 2006**
GNU tar 1.15.90, 1.15.1, 1.14.90, 1.15, 1.14	A buffer overflow vulnerability has been reported when handling PAX extended headers due to a boundary error, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code. GNU Mandriva Ubuntu Trustix RedHat SuSE Debian **Gentoo** Currently we are not aware of any exploits for this vulnerability.	GNU Tar PAX Remote Buffer Overflow CVE-2006-0300	3.9	Secunia Advisory: SA18973, February 22, 2006 Mandriva Security Advisory, MDKSA-2006:046, February 21, 2006 Ubuntu Security Notice, USN-257-1, February 23, 2006 Trustix Secure Linux Security Advisory, #2006-0010, February 24, 2006 RedHat Security Advisory, RHSA-2006:0232-3, March 1, 2006 SUSE Security Summary Report, SUSE-SR:2006:005, March 3, 2006 Debian Security Advisory, DSA-987-1, March 7, 2006 **Gentoo Linux Security Advisory, GLSA 200603-06, March 10, 2006**

GNU GNU Privacy Guard prior to 1.4.2.2.	A vulnerability has been reported caused due to an error in the detection of unsigned data, which could let a remote malicious user inject arbitrary data and bypass verification. Updates available Debian Gentoo Fedora SuSE Slackware RedHat There is no exploit code required.	GnuPG Unsigned Data Injection Detection CVE-2006-0049	2.3	GNU Security Advisory, March 9, 2006 Debian Security Advisory, DSA 993-1, March 10, 2006 Gentoo Linux Security Advisory, GLSA 200603-08, March 10, 2006 SUSE Security Announcement, SUSE-SA:2006:014, March 10, 2006 Slackware Security Advisory, SSA:2006-072-02, March 13, 2006 RedHat Security Advisory, RHSA-2006:0266-8, March 15, 2006
GnuPG GnuPG / gpg prior to 1.4.2.1	A vulnerability has been reported because 'gpgv' exits with a return code of 0 even if the detached signature file did not carry any signature (if 'gpgv" or "gpg --verify' is used), which could let a remote malicious user bypass security restrictions. Patches available Fedora Debian Mandriva Ubuntu Gentoo SuSE SuSE SuSE **Slackware** **RedHat** There is no exploit code required; however, a Proof of Concept exploit has been published.	GnuPG Detached Signature Verification Bypass CVE-2006-0455	4.9	GnuPG Advisory, February 15, 2006 Fedora Update Notification, FEDORA-2006-116, February 17, 2006 Debian Security Advisory, DSA-978-1, February 17, 2006 Mandriva Security Advisory, MDKSA-2006:043, February 17, 2006 Ubuntu Security Notice, USN-252-1, February 17, 2006 Gentoo Linux Security Advisory, GLSA 200602-10, February 18, 2006 SuSE Security Announcement, SUSE-SA:2006:009, February 20, 2006 SUSE Security Announcement, SUSE-SA:2006:013, March 1, 2006 SUSE Security Summary Report, SUSE-SR:2006:005, March 3, 2006 **Slackware Security Advisory, SSA:2006-072-02, March 13, 2006** **RedHat Security Advisory, RHSA-2006:0266-8, March 15, 2006**

GNU zgrep 1.2.4	A vulnerability has been reported in 'zgrep.in' due to insufficient validation of user-supplied arguments, which could let a remote malicious user execute arbitrary commands. Patent available Mandriva TurboLinux RedHat RedHat SGI Fedora SGI F5 Ubuntu Trustix Avaya FedoraLegacy SCO SCO Mandriva Mandriva **SGI** There is no exploit code required.	Gzip Zgrep Arbitrary Command Execution CVE-2005-0758	4.9	Security Tracker Alert, 1013928, May 10, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005: 092, May 19, 2005 Turbolinux Security Advisory, TLSA-2005-59, June 1, 2005 RedHat Security Advisory, RHSA-2005: 357-19, June 13, 2005 RedHat Security Advisory, RHSA-2005: 474-15, June 16, 2005 SGI Security Advisory, 20050603 -01-U, June 23, 2005 Fedora Update Notification, FEDORA-2005-471, June 27, 2005 SGI Security Advisory, 20050605 -01-U, July 12, 2005 Secunia Advisory: SA16159, July 21, 2005 Ubuntu Security Notice, USN-158-1, August 01, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0040, August 5, 2005 Avaya Security Advisory, ASA-2005-172, August 29, 2005 Fedora Legacy Update Advisory, FLSA:158801, November 14, 2005 SCO Security Advisories, SCOSA-2005.58 & SCOSA-2005.59, December 16, 2005 Mandriva Security Advisories, MDKSA-2006:026 & MDKSA-2006:027, January 30, 2006 **SGI Security Advisory, 20060301-01-U, March 8, 2006**
Himpfen Consulting PHP SimpleNEWS 1.x, SimpleNEWS MySQL 1.x	A vulnerability has been reported in 'admin.php' due to an insecure authentication process, which could let a remote malicious user bypass security restrictions. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	PHP SimpleNEWS Authentication Bypass	Not Available	Secunia Advisory: SA19195, March 10, 2006
Horde Project Horde Application Framework 3.0.9 & prior	A vulnerability has been reported in 'services/go.php' due to insufficient verification of the 'url' parameter before using in a 'readfile()' call, which could let a remote malicious user obtain sensitive information.	Horde Information Disclosure	Not Available	Secunia Advisory: SA19246, March 15, 2006

	Updates available Currently we are not aware of any exploits for this vulnerability.			
Image Magick ImageMagick 6.2.4.5	A vulnerability has been reported in the delegate code that is used by various ImageMagick utilities when handling an image filename due to an error, which could let a remote malicious user execute arbitrary commands; and a format string vulnerability has been reported when handling filenames received via command line arguments, which could let a remote malicious user execute arbitrary code. Ubuntu Debian Mandriva Gentoo RedHat Gentoo **SGI** There is no exploit code required.	ImageMagick Utilities Image Filename Remote Command Execution CVE-2005-4601 CVE-2006-0082	7 (CVE-2005-4601) 3.9 (CVE-2006-0082)	Secunia Advisory: SA18261, December 30, 2005 Ubuntu Security Notice, USN-246-1, January 24, 2006 Debian Security Advisory, DSA-957-1, January 26, 2006 Mandriva Security Advisory, MDKSA-2006:024, January 26, 2006 Gentoo Linux Security Advisory, GLSA 200602-06, February 13, 2006 RedHat Security Advisory, RHSA-2006:0178-4, February 14, 2006 Gentoo Linux Security Advisory, GLSA 200602-13, February 26, 2006 **SGI Security Advisory, 20060301-01-U, March 8, 2006**
Julian Pawlowski CAPI4HylaFAX 1.3	A vulnerability has been reported due to the insecure creation of temporary files, which could let a malicious user overwrite sensitive data or configuration files. No workaround or patch available at time of publishing. There is no exploit code required.	CAPI4HylaFAX Insecure Temporary File Creation CVE-2006-1231	1.6	Security Focus, Bugtraq ID: 17034, March 8, 2006
Laurent Duveau GuppY 4.5.11 & prior	A vulnerability has been reported in 'dwnld.php' due to insufficient sanitization of the 'pg' parameter, which could let a remote malicious user overwrite arbitrary files. Updates available Vulnerability can be exploited through use of a web client; however, a Proof of Concept exploit script, GuppY-rmt-DoS-expl.php, has been published.	GuppY Remote Directory Traversal CVE-2006-1224	1.9	KAPDA::#33 Advisory , March 10, 2006
Lincoln D. Stein Crypt::CBC 2.16 & prior	A vulnerability has been reported due to a flaw in its creation of IVs (Initialization Vectors) for ciphers with a blocksize larger than 8 when the RandonIV-style header is used, which could let a remote malicious user bypass security restrictions. Updates available **Debian** Currently we are not aware of any exploits for this vulnerability.	Lincoln D. Stein Crypt::CBC Perl Module Weak Ciphertext Security Bypass CVE-2006-0898	1.3	Secunia Advisory: SA18755, February 27, 2006 **Debian Security Advisory, DSA-996-1, March 13, 2006**
Metamail Metamail 2.7	A buffer overflow vulnerability has been reported when handling boundary headers within email messages, which could let a remote malicious user execute arbitrary code. *Note: According to Security Tracker this is a Linux/Unix vulnerability. Previously classified as multiple operating systems.* RedHat Mandriva SuSE **Debian** A Proof of Concept exploit has been published.	Metamail Remote Buffer Overflow CVE-2006-0709	7	Security Focus, Bugtraq ID: 16611, February 13, 2006 RedHat Security Advisory, RHSA-2006:0217-4, February 21, 2006 Mandriva Security Advisory, MDKSA-2006:047, February 22, 2006 SUSE Security Summary Report, SUSE-SR:2006:005, March 3, 2006 **Debian Security Advisory, DSA-995-1, March 13, 2006**

Multiple Vendors Xpdf 3.0 pl2 & pl3, 3.0 1, 3.00, 2.0-2.03, 1.0 0, 1.0 0a, 0.90-0.93; RedHat Fedora Core4, Core3, Enterprise Linux WS 4, WS 3, WS 2.1 IA64, WS 2.1, ES 4, ES 3, ES 2.1 IA64, 2.1, Enterprise Linux AS 4, AS 3, 2.1 IA64, 2.1, Desktop 4.0, 3.0, Advanced Workstation for the Itanium Processor 2.1 IA64, 2.1; teTeX 2.0.1, 2.0; Poppler poppler 0.4.2; KDE kpdf 0.5, KOffice 1.4.2 ; PDFTOHTML DFTOHTML 0.36	Multiple vulnerabilities have been reported: a heap-based buffer overflow vulnerability was reported in the 'DCTStream::read BaselineSOF()' function in 'xpdf/Stream.cc' when copying data from a PDF file, which could let a remote malicious user potentially execute arbitrary code; a buffer overflow vulnerability was reported in the 'DCTStream::read ProgressiveSOF()' function in 'xpdf/Stream.cc' when copying data from a PDF file, which could let a remote malicious user potentially execute arbitrary code; a buffer overflow vulnerability was reported in the 'StreamPredictor:: StreamPredictor()' function in 'xpdf/Stream.cc' when using the 'numComps' value to calculate the memory size, which could let a remote malicious user potentially execute arbitrary code; and a vulnerability was reported in the 'JPXStream: :readCodestream()' function in 'xpdf/JPXStream.cc' when using the 'nXTiles' and 'nYTiles' values from a PDF file to copy data from the file into allocated memory, which could let a remote malicious user potentially execute arbitrary code. Patches available Fedora RedHat KDE SUSE Ubuntu Gentoo RedHat RedHat RedHat Mandriva Debian Debian Debian Fedora SuSE RedHat SGI Debian TurboLinux Debian Debian Slackware Slackware Gentoo **SGI** Currently we are not aware of any exploits for these vulnerabilities.	Xpdf Buffer Overflows CVE-2005-3191 CVE-2005-3192 CVE-2005-3193	3.9 (CVE-2005-3191) 7 (CVE-2005-3192) 3.9 (CVE-2005-3193)	iDefense Security Advisory, December 5, 2005 Fedora Update Notifications, FEDORA-2005-1121 & 1122, December 6, 2005 RedHat Security Advisory, RHSA-2005:840-5, December 6, 2005 KDE Security Advisory, advisory-20051207-1, December 7, 2005 SUSE Security Summary Report, SUSE-SR:2005:029, December 9, 2005 Ubuntu Security Notice, USN-227-1, December 12, 2005 Gentoo Linux Security Advisory, GLSA 200512-08, December 16, 2005 RedHat Security Advisories, RHSA-2005:868-4, RHSA-2005:867-5 & RHSA-2005:878-4, December 20, 2005 Mandriva Linux Security Advisories MDKSA-2006:003-003-006, January 6, 2006 Debian Security Advisory, DSA-936-1, January 11, 2006 Debian Security Advisory, DSA-937-1, January 12, 2006 Debian Security Advisory, DSA 938-1, January 12, 2006 Fedora Update Notifications, FEDORA-2005-028 & 029, January 12, 2006 SUSE Security Summary Report, SUSE-SR:2006:001, January 13, 2006 RedHat Security Advisory, RHSA-2006:0160-14, January 19, 2006 SUSE Security Summary Report, SUSE-SR:2006:002, January 20, 2006 SGI Security Advisory, 20051201-01-U, January 20, 2006 Debian Security Advisory, DSA-950-1, January 23, 2006 Turbolinux Security Advisory, TLSA-2006-2, January 25, 2006 Debian Security Advisories, DSA-961-1 & 962-1, February 1, 2006

				Slackware Security Advisories, SSA:2006-045-04 & SSA:2006-045-09, February 14, 2006 Gentoo Linux Security Advisory, GLSA 200603-02, March 4, 2006 **SGI Security Advisory, 20060201-01-U, March 14, 2006**
Multiple Vendors Linux kernel 2.6-2.6.14	A Denial of Service vulnerability has been reported in 'net/ipv6/udp.c' due to an infinite loop error in the 'udp_v6_get_port()' function. Fedora Upgrades available Ubuntu SUSE RedHat RedHat RedHat **SmoothWall** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel IPV6 Denial of Service CVE-2005-2973	2.3	Secunia Advisory: SA17261, October 21, 2005 Fedora Update Notifications, FEDORA-2005-1007 & 1013, October 20, 2005 Security Focus, Bugtraq ID: 15156, October 31, 2005 Ubuntu Security Notice, USN-219-1, November 22, 2005 SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005 SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005 RedHat Security Advisory, RHSA-2006:0140-9, January 19, 2006 RedHat Security Advisories, RHSA-2006:0190-5 & RHSA-2006:0191-9, February 1, 2006 **SmoothWall Advisory, March 15, 2006**
Multiple Vendors Fast Lexical Analyzer Generator (Flex) prior to 2.5.33	A buffer overflow vulnerability has been reported in 'flex.skl' due to a boundary error, which could let a remote malicious user execute arbitrary code. Updates available Ubuntu Gentoo Currently we are not aware of any exploits for this vulnerability.	Flex Buffer Overflow CVE-2006-0459	Not Available	Secunia Advisory: SA19071, March 8, 2006 Ubuntu Security Notice, USN-260-1, March 06, 2006 Gentoo Linux Security Advisory, GLSA 200603-07, March 7, 2006

Multiple Vendors KDE kword 1.4.2, kpdf 3.4.3, 3.2, KOffice 1.4-1.4.2, kdegraphics 3.4.3, 3.2; Gentoo Linux	Multiple buffer and integer overflows have been reported, which could let a remote malicious user execute arbitrary code. Gentoo Ubuntu Fedora Mandriva Ubuntu Debian Debian SuSE RedHat RedHat Fedora Debian Trustix Mandriva RedHat SGI Debian TurboLinux Gentoo Debian Debian Slackware Slackware **SGI** Currently we are not aware of any exploits for this vulnerability.	KPdf & KWord Multiple Unspecified Buffer & Integer Overflow CVE-2005-3624 CVE-2005-3625 CVE-2005-3626 CVE-2005-3627	Not Available	Gentoo Linux Security Advisory GLSA 200601-02, January 5, 2006 Ubuntu Security Notice, USN-236-1, January 05, 2006 Fedora Update Notifications, FEDORA-2005-000, January 5, 2006 Mandriva Linux Security Advisories MDKSA-2006:003-003-006 & 008, January 6 & 7, 2006 Ubuntu Security Notice, USN-236-2, January 09, 2006 Debian Security Advisory DSA 931-1, January 9, 2006 Debian Security Advisory, DSA-936-1, January 11, 2006 SUSE Security Announcement, SUSE-SA:2006:001, January 11, 2006 RedHat Security Advisories, RHSA-2006:0163-2 & RHSA-2006:0177-5, January 11, 2006 Fedora Update Notifications, FEDORA-2005-028 & 029, January 12, 2006 Debian Security Advisories, DSA 937-1, 938-1, & 940-1, January 12 & 13, 2006 Trustix Secure Linux Security Advisory, 2006-0002, January 13, 2006 Mandriva Linux Security Advisory, MDKSA-2006:012, January 13, 2006 RedHat Security Advisory, RHSA-2006:0160-14, January 19, 2006 SGI Security Advisory, 20051201-01-U, January 20, 2006 Debian Security Advisory, DSA-950-1, January 23, 2006 Turbolinux Security Advisory, TLSA-2006-2, January 25, 2006 Gentoo Linux Security Advisory, GLSA 200601-17, January 30, 2006 Debian Security Advisories, DSA-961-1 & 962-1, February 1, 2006 Slackware Security Advisories, SSA:2006-045-04 &

				SSA:2006-045-09, February 14, 2006 **SGI Security Advisory, 20060201-01-U, March 14, 2006**
Multiple Vendors Linux Kernel 2.4, 2.6	A race condition vulnerability has been reported in ia32 emulation, that could let local malicious users obtain root privileges or create a buffer overflow. Patch Available Trustix SUSE RedHat Debian **SmoothWall** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Race Condition and Buffer Overflow CVE-2005-1768	5.6	Security Focus, 14205, July 11, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0036, July 14, 2005 SUSE Security Announcement, SUSE-SA:2005:044, August 4, 2005 RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005 Debian Security Advisory, DSA 921-1, December 14, 2005 **SmoothWall Advisory, March 15, 2006**
Multiple Vendors Linux kernel 2.2.x, 2.4.x, 2.6.x	A buffer overflow vulnerability has been reported in the 'elf_core_dump()' function due to a signedness error, which could let a malicious user execute arbitrary code with ROOT privileges. Update available Trustix Ubuntu RedHat Avaya SUSE Trustix Mandriva Conectiva **SmoothWall** An exploit script has been published.	Linux Kernel ELF Core Dump Buffer Overflow CVE-2005-1263	7	Secunia Advisory, SA15341, May 12, 2005 Trustix Secure Linux Security Advisory, 2005-0022, May 13, 2005 Ubuntu Security Notice, USN-131-1, May 23, 2005 RedHat Security Advisory, RHSA-2005:472-05, May 25, 2005 Avaya Security Advisory, ASA-2005-120, June 3, 2005 Trustix Secure Linux Bugfix Advisory, TSLSA-2005-0029, June 24, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:110 & 111, June 30 & July 1, 3005 Conectiva Linux Announcement, CLSA-2005:999, August 17, 2005 **SmoothWall Advisory, March 15, 2006**

Multiple Vendors Linux kernel 2.6-2.6.12, 2.4-2.4.31	A remote Denial of Service vulnerability has been reported due to a design error in the kernel. The vendor has released versions 2.6.13 and 2.4.32-rc1 of the kernel to address this issue. Ubuntu Mandriva SUSE Conectiva RedHat RedHat RedHat Mandriva **SmoothWall** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Remote Denial of Service CVE-2005-3275	3.3	Ubuntu Security Notice, USN-219-1, November 22, 2005 Mandriva Linux Security Advisories, MDKSA-2005:218, 219 & 220, November 30, 2005 SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005 Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006 RedHat Security Advisory, RHSA-2006:0140-9, January 19, 2006 RedHat Security Advisories, RHSA-2006:0190-5 & RHSA-2006:0191-9, February 1, 2006 Mandriva Security Advisory, MDKSA-2006:044, February 21, 2006 **SmoothWall Advisory, March 15, 2006**
Multiple Vendors Linux kernel 2.6-2.6.14, 2.5.0-2.5.69, 2.4-2.4.32, 2.3, 2.3.x, 2.3.99, pre1-pre7, 2.2-2.2.27, 2.1, 2.1 .x, 2.1.89, 2.0.28-2.0.39	A vulnerability has been reported due to the way console keyboard mapping is handled, which could let a malicious user modify the console keymap to include scripted macro commands. Mandriva Fedora Conectiva **SmoothWall** There is no exploit code required; however, a Proof of Concept exploit has been published.	Linux Kernel Console Keymap Arbitrary Command Injection CVE-2005-3257	4.9	Security Focus, Bugtraq ID: 15122, October 17, 2005 Mandriva Linux Security Advisories, MDKSA-2005:218, 219 & 220, November 30, 2005 Fedora Update Notification, FEDORA-2005-1138, December 13, 2005 Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006 **SmoothWall Advisory, March 15, 2006**
Multiple Vendors Linux kernel 2.6-2.6.15 .4	Multiple vulnerabilities have been reported: a Denial of Service vulnerability has been reported in the 'nfs_get_user_pages()' function due to insufficient checks on the return value; a Denial of Service vulnerability has been reported due to missing checks for bad elf entry addresses; and a Denial of Service vulnerability has been reported in the 'sys_mbind()' function due to insufficient sanity checks. Updates available Fedora **Ubuntu** There is no exploit code required.	Linux Kernel Local Denials of Service CVE-2006-0554 CVE-2006-0555 CVE-2006-0741	1 (CVE-2006-0554) 1.6 (CVE-2006-0555) 1.3 (CVE-2006-0741)	Secunia Advisory: SA19083, March 2, 2006 **Ubuntu Security Notice, USN-263-1 March 13, 2006**
Multiple Vendors Linux kernel 2.6-2.6.16 -rc1, 2.4.27	A vulnerability has been reported due to an implementation flaw of a zero IP ID information disclosure countermeasure, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Linux Kernel IP ID Information Disclosure CVE-2006-1242	Not Available	Security Focus, Bugtraq ID: 17109, March 14, 2006

Multiple Vendors MandrakeSoft Multi Network Firewall 2.0, Linux Mandrake 2006.0 x86_64, 2006.0, 10.2 x86_64, 10.2, Corporate Server 3.0 x86_64, 3.0; GNU wget 1.10; Daniel Stenberg curl 7.14.1, 7.13.1, 7.13, 7.12.1-7.12.3, 7.11-7.11.2, 7.10.6-7.10.8	A buffer overflow vulnerability has been reported due to insufficient validation of user-supplied NTLM user name data, which could let a remote malicious user execute arbitrary code. WGet Daniel Stenberg Mandriva Ubuntu Fedora Trustix Gentoo RedHat RedHat SUSE Slackware Debian **SCO** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendor WGet/Curl NTLM Username Buffer Overflow CVE-2005-3185	7	Security Tracker Alert ID: 1015056, October 13, 2005 Mandriva Linux Security Update Advisories, MDKSA-2005:182 & 183, October 13, 200 Ubuntu Security Notice, USN-205-1, October 14, 2005 Fedora Update Notifications FEDORA-2005-995 & 996, October 17, 2005 Fedora Update Notification, FEDORA-2005-1000, October 18, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005 Gentoo Linux Security Advisory. GLSA 200510-19, October 22, 2005 RedHat Security Advisories, RHSA-2005:807-6 & RHSA-2005:812-5, November 2, 2005 SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005 Slackware Security Advisory, SSA:2005-310-01, November 7, 2005 Debian Security Advisor, DSA 919-1, December 12, 2005 **SCO Security Advisory, SCOSA-2006.10, March 14, 2006**
Multiple Vendors RedHat Enterprise Linux WS 4, WS 3, 2.1, IA64, ES 4, ES 3, 2.1, IA64, AS 4, AS 3, AS 2.1, IA64, Desktop 4.0, 3.0, Advanced Workstation for the Itanium Processor 2.1, IA64; OpenSSL Project OpenSSL 0.9.3-0.9.8, 0.9.2 b, 0.9.1 c; FreeBSD 6.0 -STABLE, -RELEASE, 5.4 -RELENG, -RELEASE, 5.3 -STABLE, -RELENG, -RELEASE, 5.3, 5.2.1 -RELEASE, -RELENG, 5.2 -RELEASE, 5.2, 5.1 -RELENG, -RELEASE/Alpha, 5.1 -RELEASE-p5, -RELEASE, 5.1, 5.0 -RELENG, 5.0, 4.11 -STABLE,	A vulnerability has been reported due to the implementation of the 'SSL_OP_MSIE_ SSLV2_RSA_PADDING' option that maintains compatibility with third party software, which could let a remote malicious user bypass security. OpenSSL FreeBSD RedHat Mandriva Gentoo Slackware Fedora Sun Ubuntu OpenPKG SUSE Trustix SGI Debian	Multiple Vendors OpenSSL Insecure Protocol Negotiation CVE-2005-2969	3.3	OpenSSL Security Advisory, October 11, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:21, October 11, 2005 RedHat Security Advisory, RHSA-2005:800-8, October 11, 2005 Mandriva Security Advisory, MDKSA-2005:179, October 11, 2005 Gentoo Linux Security Advisory, GLSA 200510-11, October 12, 2005 Slackware Security Advisory, SSA:2005-286-01, October 13, 2005 Fedora Update Notifications, FEDORA-2005-985 & 986, October 13, 2005 Sun(sm) Alert Notification Sun Alert ID: 101974, October 14, 2005

-RELENG, 4.10 -RELENG, -RELEASE, 4.10	NetBSD BlueCoat Systems Debian Astaro Security Linux SCO IBM IBM IBM FedoraLegacy Cisco Avaya **SmoothWall** Currently we are not aware of any exploits for this vulnerability.			Ubuntu Security Notice, USN-204-1, October 14, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.022, October 17, 2005 SUSE Security Announcement, SUSE-SA:2005:061, October 19, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005 SGI Security Advisory, 20051003-01-U, October 26, 2005 Debian Security Advisory DSA 875-1, October 27, 2005 NetBSD Security Update, November 1, 2005 BlueCoat Systems Advisory, November 3, 2005 Debian Security Advisory, DSA 888-1, November 7, 2005 Astaro Security Linux Announcement, November 9, 2005 SCO Security Advisory, SCOSA-2005.48, November 15, 2005 IBM Documents Doc Number=2306, 2307, & 2312, December 15, 2005 Fedora Legacy Update Advisory, FLSA:166939, December 17, 2005 Cisco Security Notice, Document ID: 68324, December 19, 2005 Avaya Security Advisory, ASA-2006-031, January 30, 2006 **SmoothWall Advisory, March 15, 2006**
Multiple Vendors RedHat Fedora Core4; Linux Kernel 2.6.x	A Denial of Service vulnerability has been reported in the 'die_if_kernel()' function because it is erroneously marked with a 'noreturn' attribute. Updates available **Ubuntu** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel 'die_if_kernel()' Potential Denial of Service CVE-2006-0742	**1.4**	Security Focus, Bugtraq ID: 16993, March 5, 2006 **Ubuntu Security Notice, USN-263-1 March 13, 2006**
Multiple Vendors Ubuntu Linux 5.10 powerpc, i386, amd64, 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Linux kernel 2.6-2.6.15 .3	A race condition vulnerability has been reported in the security key functionality, which could let a malicious user cause a Denial of Service and possibly obtain sensitive information. Updates available Ubuntu Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Security Key Functions CVE-2006-0457	5.3	Security Focus, Bugtraq ID: 17084, March 13, 2006 Ubuntu Security Notice, USN-263-1 March 13, 2006

Multiple Vendors Ubuntu Linux 5.10 powerpc, i386, amd64, 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; MandrakeSoft Linux Mandrake 2006.0 x86_64, 2006.0, 10.2 x86_64, 10.2, 10.1 x86_64, 10.1, Corporate Server 3.0 x86_64, 3.0; GNU Mailman 2.1-2.1.5, 2.0-2.0.14	A remote Denial of Service vulnerability has been reported in the email date parsing functionality due to an error in the handling of dates. Mandriva Ubuntu Debian RedHat **Trustix** There is no exploit code required.	GNU Mailman Remote Denial of Service CVE-2005-4153	3.3	Security Focus, Bugtraq ID: 16248, January 16, 2006 Ubuntu Security Notice, USN-242-1 January 16, 2006 Debian Security Advisory, DSA-955-1, January 25, 2006 RedHat Security Advisory, RHSA-2006:0204-10, March 7, 2006 **Trustix Secure Linux Security Advisory #2006-0012, March 10, 2006**
PCRE PCRE 6.1, 6.0, 5.0	A vulnerability has been reported in 'pcre_compile.c' due to an integer overflow, which could let a remote/local malicious user potentially execute arbitrary code. Updates available Ubuntu Ubuntu Fedora Gentoo Mandriva SUSE Slackware Ubuntu Debian Slackware Gentoo Conectiva Gentoo Debian Gentoo Debian Conectiva TurboLinux Avaya Trustix HP Trustix Updates available **SCO** Currently we are not aware of any exploits for this vulnerability.	PCRE Regular Expression Heap Overflow CVE-2005-2491	7	Secunia Advisory: SA16502, August 22, 2005 Ubuntu Security Notice, USN-173-1, August 23, 2005 Ubuntu Security Notices, USN-173-1 & 173-2, August 24, 2005 Fedora Update Notifications, FEDORA-2005-802 & 803, August 24, 2005 Gentoo Linux Security Advisory, GLSA 200508-17, August 25, 2005 Mandriva Linux Security Update Advisories, MDKSA-2005:151-155, August 25, 26, & 29, 2005 SUSE Security Announcements, SUSE-SA:2005:048 & 049, August 30, 2005 Slackware Security Advisories, SSA:2005-242-01 & 242-02, August 31, 2005 Ubuntu Security Notices, USN-173-3, 173-4 August 30 & 31, 2005 Debian Security Advisory, DSA 800-1, September 2, 2005 SUSE Security Announcement, SUSE-SA:2005:051, September 5, 2005 Slackware Security Advisory, SSA:2005-251-04, September 9, 2005 Gentoo Linux Security Advisory, GLSA 200509-08, September 12, 2005 Conectiva Linux Announcement, CLSA-2005:1009, September 13, 2005 Gentoo Linux Security Advisory, GLSA 200509-12, September 19, 2005 Debian Security Advisory, DSA 817-1 & DSA 819-1,

				September 22 & 23, 2005 Gentoo Linux Security Advisory, GLSA 200509-19, September 27, 2005 Debian Security Advisory, DSA 821-1, September 28, 2005 Conectiva Linux Announcement, CLSA-2005:1013, September 27, 2005 Turbolinux Security Advisory, TLSA-2005-92, October 3, 2005 Avaya Security Advisory, ASA-2005-216, October 18, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005 HP Security Bulletin, HPSBUX02074, November 16, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0062, November 22, 2005 Security Focus, Bugtraq ID: 14620, November 25, 2005 **SCO Security Advisory, SCOSA-2006.10, March 14, 2006**
Rahul Dhesi Zoo 2.10	A buffer overflow vulnerability has been reported in the 'fullpath()' in 'misc.c' due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code. SuSE Gentoo **Debian** Currently we are not aware of any exploits for this vulnerability.	zoo Buffer Overflow CVE-2006-0855	3.9	Security Tracker Alert ID: 1015668, February 23, 2006 SUSE Security Summary Report, SUSE-SR:2006:005, March 3, 2006 Gentoo Linux Security Advisory, GLSA 200603-05, March 6, 2006 **Debian Security Advisory, DSA 991-1, March 10, 2006**
RedHat RedHat initscripts 7.93.24, Enterprise Linux WS 4, ES 4, AS 4m Desktop 4.0	A vulnerability has been reported when the 'sbin/service' command is run due to an error when handling certain variables, which could let a malicious user obtain elevated privileges. Updates available Currently we are not aware of any exploits for this vulnerability.	Red Hat Initscripts Elevated Privileges CVE-2005-3629	Not Available	RedHat Security Advisory, RHSA-2006:0016-18, March 7, 2006
sa-exim sa-exim 4.0-4.2	A vulnerability has been reported in 'greylistclean.cron' when deleting files containing spaces in their filenames in the greylist cache directory, which could let a remote malicious user bypass security restrictions. Updates available Currently we are not aware of any exploits for this vulnerability.	sa-exim Security Restriction Bypass	Not Available	Security Focus, Bugtraq ID: 17110, March 14, 2006

Ubuntu Ubuntu Linux 5.10 powerpc, i386, amd64	A vulnerability has been reported because user credentials are written to world-readable installation log files during installation, which could let a malicious user obtain sensitive information Updates available There is no exploit code required.	Ubuntu Linux Installation Password Disclosure CVE-2006-1183	7	Ubuntu Security Notice, USN-262-1 March 12, 2006

[back to top]

Multiple Operating Systems - Windows/UNIX/Linux/Other

Vendor & Software Name	Description	Common Name	CVSS	Resources
Adobe Flash Player 8.0.22.0 and prior, Breeze Meeting Add-In 5.1 and prior, Shockwave Player 10.1.0.11 and prior, Flash Debug Player 7.0.14.0 and prior	A vulnerability has been reported in Flash Player that could let remote malicious users execute arbitrary code. Adobe (formerly Macromedia) Currently we are not aware of any exploits for these vulnerabilities.	Flash Player Arbitrary Code Execution CVE-2006-0024	7	Adobe, Security Bulletin APSB06-03, March 14, 2006
Apache	A vulnerability has been reported in Apache which can be exploited by remote malicious users to smuggle http requests. Conectiva Fedora Mandriva Ubuntu TurboLinux SGI SuSE Debian Ubuntu SGI IBM has released fixes for Hardware Management Console addressing this issue. Users should contact IBM for further information. Trustix Slackware HP **SmoothWall** Currently we are not aware of any exploits for this vulnerability.	Apache HTTP Request Smuggling Vulnerability CVE-2005-1268 CVE-2005-2088	3.3 (CVE-2005-1268) 3.3 (CVE-2005-2088)	Secunia, Advisory: SA14530, July 26, 2005 Conectiva, CLSA-2005:982, July 25, 2005 Fedora Update Notification FEDORA-2005-638 & 639, August 2, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:129, August 3, 2005 Ubuntu Security Notice, USN-160-1, August 04, 2005 Turbolinux Security Advisory, TLSA-2005-81, August 9, 2005 SGI Security Advisory, 20050802-01-U, August 15, 2005 SUSE Security Announcement, SUSE-SA:2005:046, August 16, 2005 Debian Security Advisory DSA 803-1, September 8, 2005 Ubuntu Security Notice, USN-160-2, September 07, 2005 SGI Security Advisory, 20050901-01-U, September 7, 2005 Security Focus, Bugtraq ID: 14106, September 21, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005 Slackware Security Advisory,

				SSA:2005-310-04, November 7, 2005 HP Security Bulletin, HPSBUX02074, November 16, 2005 **SmoothWall Advisory, March 15, 2006**
Apache Software Foundation libapreq2 2.0.6	A remote Denial of Service vulnerability has been reported due to errors in the 'apreq_parse_headers()' and 'apreq_parse_urlencoded()' functions. Update available **Debian** Currently we are not aware of any exploits for this vulnerability.	Apache Libapreq2 Remote Denial of Service CVE-2006-0042	2.3	Security Focus, Bugtraq ID: 16710, February 17, 2006 **Debian Security Advisory, DSA-1000-1, March 14, 2006**
Apple QuickTime Player 7.0.4, 7.0.3, iTunes 6.0.2, 6.0.1	An integer overflow and heap-based buffer overflow vulnerability have been reported in Apple QuickTime and iTunes, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required.	Apple QuickTime/iTunes Integer & Heap Overflow	Not Available	Security Focus, Bugtraq ID: 17074, March 11, 2006
Belchior Foundry vCard 2.9, 2.8	Cross-Site Scripting vulnerabilities have been reported in 'create.php' due to insufficient sanitization of the 'card_id,' 'uploaded,' 'card_fontsize,' and 'card_color' parameters before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, a Proof of Concept exploit has been published.	vCard Cross-Site Scripting CVE-2006-1230	2.3	Security Focus, Bugtraq ID: 17073, March 11, 2006
bespin.org Enet Jun.2005, Jul.2005	Several vulnerabilities have been reported: a remote Denial of Service vulnerability was reported in the 'enet_protocol_handle_ incoming_commands()' function when validating a pointer; and a remote Denial of Service vulnerability was reported when handling fragmented packet reassembly. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script, enet_exploit.c, has been published.	ENet Remote Denials of Service CVE-2006-1194 CVE-2006-1195	2.3 (CVE-2006-1194) 2.3 (CVE-2006-1195)	Secunia Advisory: SA19208, March 13, 2006
BomberClone BomberClone prior to 0.11.6.2; Gentoo Linux	A buffer overflow vulnerability has been reported due to a boundary error when processing error messages, which could let a remote malicious user execute arbitrary code. Gentoo **Debian** Currently we are not aware of any exploits for this vulnerability.	BomberClone Error Messages Buffer Overflow CVE-2006-0460	7	Security Focus, Bugtraq ID: 16697, February 17, 2006 Gentoo Linux Security Advisory, GLSA 200602-09, February 16, 2006 **Debian Security Advisory, DSA-997-1, March 13, 2006**
CoreNews CoreNews 2.0.1	A vulnerability has been reported in 'index.php' which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. Vulnerability can be exploited via a web client; however, a Proof of Concept exploit has been published.	Core News Remote Code Execution CVE-2006-1212	7	Security Focus, Bugtraq ID: 17067, March 10, 2006
D2K Soft D2KBlog 1.0.3 & prior	Multiple vulnerabilities have been reported: an SQL injection vulnerability was reported due to insufficient sanitization of the 'memName' cookie parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a script insertion vulnerability was reported due to insufficient sanitization of the 'msg' parameter when	D2KBlog Script Insertion & SQL Injection CVE-2006-1122 CVE-2006-1123	10 (CVE-2006-1122) 10 (CVE-2006-1123)	KAPDA::#32 Advisory, March 1, 2006

	signing the guestbook before using, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited with a web client.; however, a Proof of Concept exploit script, d2kblog-sql-inj.pl, has been published.			
DCP-Portal DCP-Portal 6.1.1, 6.1, 6.0, 5.3-5.3.2, 5.2, 5.1, 5.0.2, 5.0.1, 4.5.1, 4.2, 4.1, 4.0, 3.7	Multiple Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through use of a web client; however, Proof of Concept exploits have been published.	DCP Portal Multiple Cross-Site Scripting CVE-2006-1120	1.9	Technical University of Vienna Security Advisory TUVSA-0603-001, March 9, 2006
Drupal Drupal prior to 4.5.8 & 4.6.6	Multiple vulnerabilities have been reported: a vulnerability was reported when using 'menu.module' to create a menu item, which could let a remote malicious user bypass security restrictions; a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of unspecified input before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability was reported when handling sessions during login due to an error, which could let a remote malicious user hijack another user's session; and a vulnerability was reported due to insufficient sanitization of unspecified input before using in mail headers, which could let a remote malicious user inject arbitrary headers in outgoing mails. Updates available Vulnerabilities can be exploited through a web client.	Drupal Multiple Vulnerabilities CVE-2006-1225 CVE-2006-1226 CVE-2006-1227 CVE-2006-1228	7 (CVE-2006-1225) 2.3 (CVE-2006-1226) 1.6 (CVE-2006-1227) 5.6 (CVE-2006-1228)	Secunia Advisory: SA19245, March 14, 2006
DSPortal DSCounter 1.2	An SQL injection vulnerability has been reported in the 'index.php' script due to insufficient validation of the 'X-Forwarded-For' HTTP header parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	DSCounter SQL Injection CVE-2006-1234	5.6	Security Tracker Alert ID: 1015756, March 13, 2006
DSPortal DSNewsletter 1.1	An SQL injection vulnerability has been reported due to insufficient sanitization of the 'email' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client.	DSNewsletter SQL Injection CVE-2006-1237	7	Security Tracker Alert ID: 1015757, March 13, 2006
DSPortal DSPoll 1.1	An SQL injection vulnerability has been reported in the 'pollid' parameter due to insufficient sanitization before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client.	DSPoll SQL Injection CVE-2006-1217	7	Security Tracker Alert ID: 1015758, March 13, 2006
DSPortal DSDownload 1.0	SQL injection vulnerabilities have been reported in 'downloads.php' due to insufficient sanitization of the 'category' parameter and in 'search.php' due to insufficient sanitization of the 'key' parameter, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for these vulnerabilities.	DSDownload Multiple SQL Injection CVE-2006-1232	1.9	Security Tracker Alert ID: 1015755, March 13, 2006

Ethereal Group Ethereal 0.10-0.10.13, 0.9-0.9.16, 0.8.19, 0.8.18, 0.8.13-0.8.15, 0.8.5, 0.8, 0.7.7	A buffer overflow vulnerability has been reported in the 'dissect_ospf_ v3_address_ prefix()' function in the OSPF protocol dissector due to a boundary error when converting received binary data to a human readable string, which could let a remote malicious user execute arbitrary code. Patch available Debian Gentoo Mandriva Fedora RedHat Avaya SuSE **SGI** Currently we are not aware of any exploits for this vulnerability.	Ethereal OSPF Protocol Dissection Buffer Overflow CVE-2005-3651	7	iDefense Security Advisory, December 9, 2005 Debian Security Advisory DSA 920-1, December 13, 2005 Gentoo Linux Security Advisory, GLSA 200512-06, December 14, 2005 Mandriva Linux Security Advisory MDKSA-2005:227, December 15, 2005 Mandriva Linux Security Advisory MDKSA-2006:002, January 3, 2006 Fedora Update Notification FEDORA-2005-000, January 5, 2006 RedHat Security Advisory, RHSA-2006:0156-6, January 11, 2006 Avaya Security Advisory, ASA-2006-046, February 13, 2006 SUSE Security Summary Report, SUSE-SR:2006:004, February 24, 2006 **SGI Security Advisory, 20060201-01-U, March 14, 2006**
Ethereal Group Ethereal 0.9.1-0.10.13.	A remote Denial of Service vulnerability has been reported in the IRC and GTP dissectors when a malicious user submits a specially crafted packet. Upgrades available Mandriva RedHat Avaya SuSE **SGI** Currently we are not aware of any exploits for this vulnerability.	Ethereal IRC & GTP Dissectors Remote Denial of Service CVE-2005-4585	3.3	Ethereal Security Advisory, enpa-sa-00022, December 27, 2005 Mandriva Linux Security Advisory MDKSA-2006:002, January 3, 2006 RedHat Security Advisory, RHSA-2006:0156-6, January 11, 2006 Avaya Security Advisory, ASA-2006-046, February 13, 2006 SUSE Security Summary Report, SUSE-SR:2006:004, February 24, 2006 **SGI Security Advisory, 20060201-01-U, March 14, 2006**
FFmpeg FFmpeg 0.4.9 -pre1, 0.4.6-0.4.8, FFmpeg CVS	A buffer overflow vulnerability has been reported in the 'avcodec_default_get_buffer()' function of 'utils.c' in libavcodec due to a boundary error, which could let a remote malicious user execute arbitrary code. Patches available Ubuntu Mandriva Ubuntu	FFmpeg Remote Buffer Overflow CVE-2005-4048	7	Secunia Advisory: SA17892, December 6, 2005 Ubuntu Security Notice, USN-230-1, December 14, 2005 Mandriva Linux Security Advisories MDKSA-2005:228-232, December 15, 2005

	Gentoo Gentoo **Debian** Currently we are not aware of any exploits for this vulnerability.			Ubuntu Security Notice, USN-230-2, December 16, 2005 Gentoo Linux Security Advisory, GLSA 200602-01, February 5, 2006 Gentoo Linux Security Advisory, GLSA 200603-03, March 4, 2006 **Debian Security Advisory, DSA-992-1, March 10, 2006**
free-av.de AntiVir Personal Edition Classic 7	A vulnerability has been in 'notepad' because the application is run with SYSTEM privileges when clicking on the 'Report' button after an update is completed, which could let a malicious user obtain elevated privileges. No workaround or patch available at time of publishing. There is no exploit code required.	AntiVir Update Report Elevated Privileges	Not Available	Secunia Advisory: SA19217, March 13, 2006
Gallery Project Gallery 2.0.3 & prior	A file include vulnerability has been reported in 'upgrade/index.php' and 'install/index.php' due to insufficient verification of the 'stepOrder[]' parameter before using to include files, which could let a remote malicious user include arbitrary files and execute arbitrary PHP code. No workaround or patch available at time of publishing. A Proof of Concept exploit script, gallery_stepOrder_ watermark.php, has been published.	Gallery File Include CVE-2006-1219	2.3	Secunia Advisory: SA19175 , March 9, 2006
GGZ Gaming Zone GGZ Gaming Zone 0.0.12 & prior	A remote Denial of Service vulnerability has been reported due to an error in the client when handling malformed XML data. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script, ggzcdos.c, has been published.	GGZ Gaming Remote Denial of Service	Not Available	Secunia Advisory: SA19212, March 13, 2006
Gnome Ltd. Dwarf HTTP Server 1.3.2	Several vulnerabilities have been reported: a vulnerability was reported due to a validation error in the filename extension supplied by the user in the URL, which could let a remote malicious user obtain sensitive information; and a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of input passed to the URL before returning to the user in an error message, which could let a remote malicious user execute arbitrary HTML and script code. Updates available Currently we are not aware of any exploits for these vulnerabilities.	Dwarf HTTP Server Information Disclosure & Cross-Site Scripting CVE-2006-0819 CVE-2006-0820	3.3 (CVE-2006-0819) 2.3 (CVE-2006-0820)	Secunia Advisory: SA18962, March 13, 2006
IBM Tivoli Lightweight Client Framework 3.7.1	A vulnerability has been reported in the HTTP interface of Tivoli LCF (Lightweight Client Framework), which could let a remote malicious user obtain sensitive information. Workaround information Currently we are not aware of any exploits for this vulnerability.	IBM Tivoli Lightweight Client Framework Information Disclosure CVE-2000-1239	Not Available	Security Focus, Bugtraq ID: 17085, March 13, 2006
Jcink textfileBB 1.0	A Cross-Site Scripting vulnerability has been reported in 'messanger.php' due to insufficient sanitization of the 'mess' and 'user' parameters before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	Jcink TextfileBB Cross-Site Scripting CVE-2006-1202	2.3	Security Tracker Alert ID: 1015744 , March 9, 2006

Jupiter CMS Jupiter CMS 1.1.5, 1.1.4	An HTML injection vulnerability has been reported in the 'image' BBcode due to insufficient sanitization of user-supplied input before using it in dynamically generated content, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through use of a web client; however, exploit details, JupiterCMS.txt, have been published.	Jupiter CMS BBCode HTML Injection CVE-2006-1223	2.3	Security Focus, Bugtraq ID: 17072, March 11, 2006
Light Weight Calendar Light Weight Calendar 1.0	A vulnerability has been reported in 'index.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script, lwc_rce_index.php.pl, has been published.	Light Weight Calendar Remote Command Execution	Not Available	Security Focus, Bugtraq ID: 17059, March 9, 2006
L-Soft Listserv 14.4, 14.3	Multiple unspecified vulnerabilities have been reported which could let a remote malicious user execute arbitrary code. Updates available Currently we are not aware of any exploits for these vulnerabilities.	L-Soft Listserv Multiple Unspecified Vulnerabilities CVE-2006-1044	7	NGSSoftware Insight Security Research Advisory , March 4, 2006 **US-CERT VU#841132**
Lurker Lurker 2.0 & prior	Multiple vulnerabilities have been reported: an input validation vulnerability was reported in 'lurker.cgi,' which could let a remote malicious user obtain sensitive information; a vulnerability was reported due to an unspecified error which could let a remote malicious user create or overwrite arbitrary files in any directory called 'mbox;' and a vulnerability was reported due to insufficient sanitization of unspecified input before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. Updates available **Debian** Vulnerabilities can be exploited through use of a web client.	Lurker Multiple Vulnerabilities CVE-2006-1062 CVE-2006-1063 CVE-2006-1064	2.3 (CVE-2006-1062) 2.3 (CVE-2006-1063) **1.9** (CVE-2006-1064)	Secunia Advisory: SA19136, March 6, 2006 **Debian Security Advisory, DSA-999-1, March 14, 2006**
manas tungare Site Membership manas tungare Site Membership Script 0	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'login.asp' and 'default.asp' due to insufficient sanitization of the 'Error' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; and an SQL injection vulnerability was reported in 'login.asp' due to insufficient sanitization of the 'username' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Updates available Vulnerabilities can be exploited through use of a web client.	manas tungare Site Membership Script Cross-Site Scripting & SQL Injection CVE-2006-1155 CVE-2006-1156	2.3 (CVE-2006-1155) 2.3 (CVE-2006-1156)	Secunia Advisory: SA19156, March 9, 2006
Mikael Software WMNews 0	Cross-Site Scripting vulnerabilities has been reported in 'vmview.php' due to insufficient sanitization of the 'ArtCat' parameter, in 'foot.php' due to insufficient sanitization the 'ctrrowcol' parameter and in 'wmcomments.php' due to insufficient sanitization of the 'ArtID' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client.	WMNews Multiple Cross-Site Scripting CVE-2006-1233	2.3	Secunia Advisory: SA19204, March 13, 2006

Mozilla Firefox 1.5, Netscape Browser 8.0.4; Netscape Browser 8.0.4	A remote Denial of Service vulnerability has been reported when handling large history information. *Note: The vendor disputes this claim.* Netscape Mozilla RedHat RedHat Fedora Mandriva Mandriva **SGI** A Proof of Concept exploit script has been published.	Mozilla History File Remote Denial of Service CVE-2005-4134	2.3	Secunia Advisory: SA17934, December 8, 2005 Security Focus, Bugtraq ID: 15773, January 27, 2006 Mozilla Foundation Security Advisory 2006-03, February 1, 2006 RedHat Security Advisories, RHSA-2006-0199 & RHSA-2006:0200-8, February 2, 2006 RedHat Fedora Security Advisories, FEDORA-2006-075 & FEDORA-2006-076, February 3, 2006 Mandriva Security Advisories, MDKSA-2006:036 & MDKSA-2006:037, February 7, 2006 **SGI Security Advisory, 20060201-01-U, March 14, 2006**
Multiple Vendors MandrakeSoft Linux Mandrake 2006.0 x86_64, 2006.0, 10.2 x86_64, 10.2; Gentoo Linux; Ethereal Group Ethereal 0.10.1-0.10.13, 0.9-0.9.16, 0.8.19, 0.8.18, 0.8.13-0.8.15, 0.8.5, 0.8, 0.7.7	A vulnerability has been reported in Ethereal IRC Protocol Dissector, that could let remote malicious users cause a Denial of Service. Mandriva Gentoo SUSE Conectiva Mandriva Avaya SuSE **SGI** Currently we are not aware of any exploits for this vulnerability.	Ethereal Denial of Service CVE-2005-3313	3.3	Mandriva Linux Security Advisory, MDKSA-2005:193-1, October 26, 2005 Gentoo Linux Security Advisor, GLSA 200510-25, October 30, 2005 SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005 Conectiva Security Announcement, CLSA-2005:1043, November 8, 2005 Mandriva Linux Security Advisory MDKSA-2006:002, January 3, 2006 Avaya Security Advisory, ASA-2006-046, February 13, 2006 SUSE Security Summary Report, SUSE-SR:2006:005, March 3, 2006 **SGI Security Advisory, 20060201-01-U, March 14, 2006**
Multiple Vendors Mozilla Browser 0.8-0.9.9, 0.9.35, 0.9.48, 1.0-1.7.12, Thunderbird 0.x, 1.x, Firefox 0.x, 1.x; SeaMonkey 1.0; RedHat Enterprise Linux WS 4, WS 3, WS 2.1 IA64, WS 2.1, ES 4, ES 3, ES 2.1 IA64, ES 2.1, AS 4, AS 3, AS 2.1	Multiple vulnerabilities have been reported: vulnerabilities were reported because temporary variables that are not properly protected are used in the JavaScript engine's garbage collection, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a vulnerability was reported because a remote malicious user can create HTML that will dynamically change the style of an element from position:relative to position:static; a vulnerability was reported because a remote malicious user can create HTML that invokes the QueryInterface() method of the built-in Location and Navigator objects; a vulnerability was reported in the 'XULDocument.persist()' function due to improper	Multiple Mozilla Products Vulnerabilities CVE-2006-0292 CVE-2006-0293 CVE-2006-0294 CVE-2006-0295 CVE-2006-0296 CVE-2006-0297 CVE-2006-0298 CVE-2006-0299	7 (CVE-2006-0292) 7 (CVE-2006-0293) 7 (CVE-2006-0294) 3.9 (CVE-2006-0295) 2.3	Mozilla Foundation Security Advisories 2006-01-2006-08, February 1, 2006 RedHat Security Advisories, RHSA-2006:0199-10 & RHSA-2006:0200-8, February 2, 2006 Fedora Security Advisories, FEDORA-2006-075 &

IA64, AS 2.1, Desktop 4.0, 3.0, Advanced Workstation for the Itanium Processor 2.1 IA64, 2.1	validation of the user-supplied attribute name, which could let a remote malicious user execute arbitrary code; an integer overflow vulnerability was reported in the 'E4X,' 'SVG,' and 'Canvas' features, which could let a remote malicious user execute arbitrary code; a vulnerability was reported in the XML parser because data can be read from locations beyond the end of the buffer, which could lead to a Denial of Service; and a vulnerability was reported because the 'E4X' implementation's internal 'AnyName' object is incorrectly available to web content, which could let a remote malicious user bypass same-origin restrictions. Mozilla RedHat RedHat Fedora Mandriva Mandriva **SGI** There is no exploit code required for some of these vulnerabilities; however, an exploit, firefox_queryinterface.pm, has been published.		(CVE-2006-0296) **3.9** (CVE-2006-0297) 2.3 (CVE-2006-0298) 4.7 (CVE-2006-0299)	FEDORA-2006-076, February 2, 2006 US-CERT VU#592425 US-CERT VU#759273 Mandriva Security Advisories, MDKSA-2006:036 & MDKSA-2006:037, February 7, 2006 **SGI Security Advisory, 20060201-01-U, March 14, 2006**
myBloggie myBloggie 2.1.3 Beta, 2.1.3, 2.1.2	Multiple Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through use of a web client; however, Proof of Concept exploits have been published.	MyBloggie Multiple Cross-Site Scripting CVE-2006-1205	2.3	Technical University of Vienna Security Advisory TUVSA-0603-002, March 9, 2006
Nodez Project Nodez 4.6.1.1 & prior	Several vulnerabilities have been reported: a file include vulnerability was reported due to insufficient verification of the 'op' parameter, which could let a remote malicious user execute arbitrary PHP code; and a Cross-Site Scripting vulnerability was reported in the 'op' parameter due to insufficient sanitization before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through use of a web client; however, Proof of Concept exploits have been published.	Nodez File Inclusion & Cross-Site Scripting CVE-2006-1162 CVE-2006-1163	5.6 (CVE-2006-1162) 7 (CVE-2006-1163)	Security Tracker Alert ID: 1015747, March 10, 2006
NZEO Zeroboard 4.1 pl 7 released 2005-04-04 & prior	Multiple HTML injection vulnerabilities have been reported due to insufficient sanitization of the memo subject, user email address, and the user homepage field before saving, which could let a remote malicious user execute arbitrary HTML and script code. Patches available Vulnerabilities can be exploited through use of a web client.	Zeroboard Multiple HTML Injection CVE-2006-1222	2.3	Secunia Advisory: SA19214, March 13, 2006
peer cast.org PeerCast prior to 0.1217	A buffer overflow vulnerability has been reported when handling parameters received in an URL due to a boundary error, which could let a remote malicious user execute arbitrary code. Updates available A Proof of Concept exploit script, prdelka-vs-GNU-peercast.c, has been published.	Peercast.org PeerCast Remote Buffer Overflow CVE-2006-1148	7	Security Focus, Bugtraq ID: 17040, March 9, 2006
PHP PHP 5.1.1, 5.1	Several vulnerabilities have been reported: a vulnerability was reported due to insufficient of the session ID in the session extension before returning to the user, which could let a remote malicious user inject arbitrary HTTP headers; a format string vulnerability was reported in the 'mysqli' extension when processing error messages, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported due to insufficient sanitization of unspecified input that is passed under certain error conditions,	Multiple PHP Vulnerabilities CVE-2006-0207 CVE-2006-0208	2.3 (CVE-2006-0208)	Secunia Advisory: SA18431, January 13, 2006 Mandriva Security Advisory, MDKSA-2006:028, February 1, 2006 **Ubuntu Security**

	which could let a remote malicious user execute arbitrary HTML and script code. PHP Mandriva **Ubuntu** There is no exploit code required.			**Notice, USN-261-1, March 10, 2006**
QwikiWiki QwikiWiki 1.5, 1.4	Cross-Site Scripting vulnerabilities have been reported in 'index.php,' 'login.php,' 'pageindex.php,' and 'recentchanges.php' due to insufficient sanitization of user-supplied input before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through use of a web client; however, Proof of Concept exploits have been published.	QwikiWiki Multiple Cross-Site Scripting CVE-2006-1196	2.3	Secunia Advisory: SA19182, March 10, 2006
Red BLoG RedBLoG 0.5	An SQL injection vulnerability has been reported in 'rss.php' due to insufficient sanitization of the 'cat_id' parameter before using in SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit script, redblog-05-exploit.php, has been published.	Redblog SQL Injection CVE-2006-1140	7	Security Focus, Bugtraq ID: 17041, March 9, 2006
Sauer braten Sauerbraten 2006_02_28, Sauerbraten Cube 2005_08_09	Multiple vulnerabilities have been reported including a buffer overflow vulnerability and several Denials of Service, which could let a remote malicious user execute arbitrary machine code or crash both clients and servers. **Gentoo** Exploit scripts, sauerburn.zip and evilcube.c, have been published.	Sauerbraten Multiple Remote Vulnerabilities CVE-2006-1100 CVE-2006-1101 CVE-2006-1102 CVE-2006-1103	**7** (CVE-2006-1100) **2.3** (CVE-2006-1101) **2.3** (CVE-2006-1102) **2.3** (CVE-2006-1103)	Security Focus, Bugtraq ID: 16986, March 6, 2006 **Gentoo Linux Security Advisory, GLSA 200603-10, March 13, 2006**
sBlog sBlog 0.7.2	Multiple vulnerabilities have been reported: a vulnerability was reported in 'search.php' due to insufficient sanitization of the 'keyword' parameter in an HTTP POST request, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported due to insufficient sanitization of the 'username' form field when posting a comment, which could let a remote malicious user execute arbitrary HTML and script code. Update available Vulnerabilities may be triggered through the use of a web browser application; however, Proof of Concept exploits have been published.	sBlog Multiple Vulnerabilities CVE-2006-1135	2.3	Secunia Advisory: SA19151, March 8, 2006
Simple PHP Blog Simple PHP Blog 0.4.7.1 & prior	A file include vulnerability has been reported in 'install05.php,' which could let a malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script, simple_php_ blog.0.4.7.1_file_include.pl, has been published.	Simple PHP Blog File Include CVE-2006-1243	Not Available	Security Focus, Bugtraq ID: 17102, March 14, 2006

SquirrelMail Development Team SquirrelMail 1.4.5 & prior	Multiple vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'webmail.php' due to insufficient sanitization of the 'right_main' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of input passed to comments in styles before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in the 'sqimap_mailbox_select mailbox' parameter due to insufficient sanitization before using in an IMAP query, which could let a remote malicious user inject arbitrary IMAP commands. The vulnerabilities have been fixed in the CVS repository and fixes will be included in the upcoming 1.4.6 version. Mandriva Fedora SuSE **Debian** **Gentoo** There is no exploit code required.	SquirrelMail Multiple Cross-Site Scripting & IMAP Injection CVE-2006-0188 CVE-2006-0195 CVE-2006-0377	2.3 (CVE-2006-0188) 2.3 (CVE-2006-0195) 2.3 (CVE-2006-0377)	Secunia Advisory: SA18985, February 22, 2006 Mandriva Linux Security Advisory, MDKSA-2006:049, February 27, 2006 Fedora Update Notification, FEDORA-2006-133, March 3, 2006 SUSE Security Summary Report, SUSE-SR:2006:005, March 3, 2006 **Debian Security Advisory DSA-988-1, March 8, 2006** **Gentoo Linux Security Advisory, GLSA 200603-09, March 12, 2006**
txtForum txtForum 1.0.4 -dev, 1.0.3 -dev	Multiple Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through use of a web client; however, Proof of Concept exploits have been published.	txtForum Multiple Cross-Site Scripting CVE-2006-1204	2.3	Technical University of Vienna Security Advisory TUVSA-0603-003, March 9, 2006
txtForum txtForum 1.0.4 -dev & prior	A vulnerability has been reported in 'common.php' which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. Vulnerability can be exploited through use of a web client; however, a Proof of Concept exploit has been published.	txtForum Remote PHP Code Execution CVE-2006-1203	7	Technical University of Vienna Security Advisory TUVSA-0603-004, March 9, 2006
unalz unalz 0.53	A Directory Traversal vulnerability has been reported due to an input validation error when extracting an ALZ archive, which could let a remote malicious user obtain sensitive information. Update available There is no exploit code required.	unalz Directory Traversal CVE-2006-0950	1.9	Secunia Advisory: SA19063, March 13, 2006
Unreal UnrealIRCd 3.2-3.2.3, 3.1.3, 3.1.1	A remote Denial of Service vulnerability has been reported when handling the TKL command due to an error. Updates available A Proof of Concept exploit script, UnrealIRCd-TKL-expl.pl, has been published.	UnrealIRCd Remote Denial of Service CVE-2006-1214	2.3	Secunia Advisory: SA19188, March 10, 2006
UPDI Network Enterprise @1 File Store 2006.3.7	Several vulnerabilities have been reported: an HTML injection vulnerability was reported in 'signup.php' due to insufficient sanitization of the 'real_name,' 'email,' and 'login' parameters before using, which could let a remote malicious user execute arbitrary HTML and script code; and an SQL injection vulnerability was reported in 'password.php' due to insufficient sanitization of the 'email' parameter and in various scripts due to insufficient sanitization of the 'id' parameter, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through use of a web client.	@1 File Store HTML Injection & SQL Injection	Not Available	Security Focus, Bugtraq ID: 17090, March 14, 2006

Vegas Forum Vegas Forum 1.0	An SQL injection vulnerability has been reported in 'forumlib.php' due to insufficient sanitization, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	Vegas Forum SQL Injection CVE-2006-1020	7	Security Focus, Bugtraq ID: 17079, March 13, 2006
Vz Scripts ADP Forum 2.0.3 & prior	An HTML injection vulnerability has been reported due to insufficient sanitization of the subject field, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited with a web browser; however, a Proof of Concept exploit has been published.	ADP Forum HTML Injection CVE-2006-1157	2.3	Security Focus, Bugtraq ID: 17047, March 9, 2006
W3C Libwww 5.4	Multiple unspecified vulnerabilities have been reported including a buffer overflow and vulnerabilities related to the handling of multipart/byteranges content. The impact was not specified. Fedora Mandriva Ubuntu **SCO** Currently we are not aware of any exploits for these vulnerabilities.	W3C Libwww Multiple Unspecified Vulnerabilities CVE-2005-3183	3.3	Fedora Update Notifications, FEDORA- 2005-952 & 953, October 7, 2005 Mandriva Linux Security Advisory, MDKSA-2005:210, November 10, 2005 Ubuntu Security Notice, USN-220-1, December 01, 2005 **SCO Security Advisory, SCOSA-2006.10, March 14, 2006**
Web Calendar Web Calendar 1.0.1	Several vulnerabilities have been reported: SQL injection vulnerabilities were reported due to insufficient sanitization of 'export_handler.php,' 'activity_log.php,' 'admin_handler.php,' and 'edit_template.php' before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability was reported in 'export_handler.php' due to insufficient verification of the 'id' and 'format' parameters before used to save data files, which could let a remote malicious user overwrite saved data files. **Debian** There is no exploit code required.	WebCalendar SQL Injection & File Overwrite CVE-2005-3949 CVE-2005-3961	7 (CVE-2005-3949) 2.3 (CVE-2005-3961)	Secunia Advisory: SA17784, November 29, 2005 Security Focus, Bugtraq ID: 15606, December 1, 2005 **Debian Security Advisory, DSA-1002-1, March 15, 2006**
Web Calendar WebCalendar 1.0.1	An HTTP response splitting vulnerability has been reported in 'Layers_Toggle.php' due to insufficient sanitization, which could let a remote malicious user influence or misrepresent how Web content is served, cached or interpreted. Patches available **Debian** There is no exploit code required; however, a Proof of Concept exploit has been published.	WebCalendar HTTP Response Splitting CVE-2005-3982	Not Available	Security Focus, 15673, December 1, 2005 **Debian Security Advisory, DSA-1002-1, March 15, 2006**
Xpdf Xpdf 3.01	A heap-based buffer overflow vulnerability has been reported when handling PDF splash images with overly large dimensions, which could let a remote malicious user execute arbitrary code. Gentoo Fedora RedHat RedHat Ubuntu Debian Debian	Xpdf PDF Splash Remote Buffer Overflow CVE-2006-0301	7	Secunia Advisory: SA18677, February 1, 2006 Gentoo Linux Security Advisories, GLSA 200602-04 & GLSA 200602-05, February 12, 2006 Fedora Update Notifications, FEDORA-2006-103, FEDORA-2006-104, & FEDORA-2006-105, February 10, 2006 RedHat Security Advisories,

	Debian Slackware Slackware Gentoo **Debian** Currently we are not aware of any exploits for this vulnerability.			RHSA-2006:0201-3 & RHSA-2006:0206-3, February 13, 2006 Ubuntu Security Notice, USN-249-1, February 13, 2006 Debian Security Advisories, DSA-971-1, DSA-972-1 & DSA-974-1, February 14 & 15, 2006 Slackware Security Advisories, SSA:2006-045-04& SSA:2006-045-09, February 14, 2006 Gentoo Linux Security Advisory, GLSA 200602-12, February 21, 2006 **Debian Security Advisory, DSA-998-1, March 14, 2006**
Zoph Zoph 0.x	SQL injection vulnerabilities have been reported due to insufficient sanitization of unspecified input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. The vulnerabilities have been fixed in version 0.5pre1. **Debian** There is no exploit code required.	Zoph SQL Injection CVE-2006-0402	7	Secunia Advisory: SA18563, January 23, 2006 **Debian Security Advisory, DSA 989-1, March 9, 2006**

[back to top]

Wireless Trends & Vulnerabilities

This section contains wireless vulnerabilities, articles, and malicious code that has been identified during the current reporting period.

- hcidump Bluetooth L2CAP Remote Denial of Service**:** Debian has released an update for the Denial of Service vulnerability in the L2CAP (Logical Link Control and Adaptation Layer Protocol) layer.
- Metro Wi-Fi Networks To Grow 8,400% By 2010: According to a report from ABI Research, by 2010 municipal Wi-Fi networks will cover 126,000 square miles (over 325,000 square km) worldwide. This is an increase from about 1,500 square miles in 2005 (3885 square kilometers). ABI says the growth of municipal Wi-Fi is being driven by several trends, including use of the wireless networks for public safety and increased efficiency.

[back to top]

General Trends

This section contains brief summaries and links to articles which discuss or present information pertinent to the cyber security community.

- Virus names likely a lost cause: In early February, antivirus firms warned customers about a computer virus programmed to delete files on the third of each month, but almost every company called the program by a different name. While this episode highlighted the continuing issues for the average Internet user, the incident became the first success for an effort to create a single identifier among responders for common threats. While consumers may have wondered about which threat to be worried about, incident response teams and information-technology managers had a single name for the attack, CME-24. The designation comes from the Common Malware Enumeration (CME) Project, an initiative spearheaded by federal contractor MITRE Corp. The project does not intend to solve the naming problem for consumers, but to provide a neutral common identifier that incident responders can use.
- Americans Want Banks To Spy On Their Accounts**:** According to a survey conducted by RSA Security, nine out of ten Americans want their banks to monitor their online accounts for signs of suspicious behavior. The poll also found that although consumers aren't seeing a rise in the number of phishing e-mails, they are increasingly wary of all electronic communiqués from their banks. According to telephone survey, 79 percent said that they were less likely to respond to e-mail from their bank because of worry over phishing scams; that's up nine points from 2004.
- The Tracks We Leave Behind: Web searches are not very private. They leave behind footprints in server logs that record their activities. The logs show the IP address of a user's computer, the date and time a visitor clicked on a Web page, the user's PC operating system and browser, and the referring URL that brought them to a site. An IP address can, with a reasonable degree of accuracy, be used to identify a user's location, through a geolocation service or an Internet service provider. When compelled by law or sometimes merely at the request of legal authorities, ISPs will identify their subscribers.
- Clever Phishers Dodge Spoofed Site Shutdowns: A new technique is being used by fraudsters in order to keep their spoofed Web sites up and running. According to RSA Security's Naftali Bennett, the senior vice president of its Cyota anti-fraud division, some phishers have started using a tactic called "smart site redirection" to stay a step ahead of the law.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Netsky-P	Win32 Worm	Stable	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared folder.
2	Zafi-B	Win32 Worm	Stable	June 2004	A mass-mailing worm that spreads via e-mail using several different languages, including English, Hungarian and Russian. When executed, the worm makes two copies of itself in the %System% directory with randomly generated file names.
3	Lovgate.w	Win32 Worm	Stable	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network.
4	Mytob-GH	Win32 Worm	Stable	November 2005	A variant of the mass-mailing worm that disables security related programs and allows other to access the infected system. This version sends itself to email addresses harvested from the system, forging the sender's address.
5	Netsky-D	Win32 Worm	Stable	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.
6	Mytob-AS	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that disables security related programs and processes, redirection various sites, and changing registry values. This version downloads code from the net and utilizes its own email engine.
7	Sober-Z	Win32 Worm	Stable	December 2005	This worm travels as an email attachment, forging the senders address, harvesting addresses from infected machines, and using its own mail engine. It further download code from the internet, installs into the registry, and reduces overall system security.
8	Mytob.C	Win32 Worm	Stable	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.
9	Zafi-D	Win32 Worm	Stable	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.
10	Mytob-BE	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability, and email to propagate. Harvesting addresses from the Windows address book, disabling antivirus, and modifying data.

Table updated March 13, 2006

[back to top]

Last updated March 16, 2006